

23857FP

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION  
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété  
Intellectuelle  
Bureau international



(43) Date de la publication internationale  
8 février 2001 (08.02.2001)

PCT

(10) Numéro de publication internationale  
**WO 01/10078 A1**

(51) Classification internationale des brevets<sup>7</sup>: H04L 9/32

(74) Mandataire: BRUYERE, Pierre; Gemplus, Parc d'activités de Gémenos, Avenue du Pic de Bertagne, F-13881 Gémenos (FR).

(21) Numéro de la demande internationale:

PCT/FR00/02024

(81) États désignés (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(22) Date de dépôt international: 12 juillet 2000 (12.07.2000)

(84) États désignés (régional): brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

(25) Langue de dépôt: français

(26) Langue de publication: français

Publiée:

— *Avec rapport de recherche internationale.*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.



(54) Title: SIGNATURE SCHEMES BASED ON DISCRETE LOGARITHM WITH PARTIAL OR TOTAL MESSAGE RECOVERY

(54) Titre: SCHEMAS DE SIGNATURE A BASE DE LOGARITHME DISCRET AVEC RECONSTITUTION PARTIELLE OU TOTALE DU MESSAGE

(57) Abstract: The invention concerns signature scheme methods whereof the security is based on the discrete logarithm problem, a first scheme for total recovery of the message, a second scheme for partial recovery of the message. The invention also concerns two techniques for reducing to a minimum the total size of the message to be transmitted and of the signature. The first technique consists in including part of the message inside the signature by appropriately selecting the random data used when the signature is generated. The second technique consists in eliminating part of the octets representing the signature, the total recovery of the signature being obtained during the second verification phase. Said schemes and said two techniques aim at reducing the overall size of the signature and of the message to be transmitted. They are therefore particularly designed to be used on portable media such as smart cards.

WO 01/10078 A1

(57) Abrégé: L'invention consiste en des procédés de schéma de signature dont la sécurité est basée sur le problème du logarithme discret, un premier schéma permettant une reconstitution totale du message, un deuxième schéma permettant une reconstitution partielle du message. L'invention consiste également en deux techniques permettant de minimiser la taille totale du message à transmettre et de la signature. La première technique consiste à inclure une partie du message à l'intérieur de la signature en choisissant convenablement les données aléatoires utilisées lors de la génération de la signature. La deuxième technique consiste à supprimer une partie des octets représentant la signature, la reconstitution complète de la signature s'effectuant durant la phase de vérification. Ces schémas et ces 2 techniques ont pour but de réduire la taille totale de la signature et du message à transmettre. Ils sont donc particulièrement destinés à être utilisés sur des supports portables de type carte à puce.

**SCHEMAS DE SIGNATURE A BASE DE  
LOGARITHME DISCRET AVEC RECONSTITUTION  
PARTIELLE OU TOTALE DU MESSAGE**

L'invention consiste en deux nouveaux schémas de signature électronique basés sur le problème du logarithme discret, le premier permettant la reconstitution totale du message, le second permettant 5 la reconstitution partielle du message, ainsi que deux techniques permettant de réduire la taille des signatures électroniques.

Une signature électronique d'un message est un nombre dépendant à la fois d'une clé secrète connue 10 seulement de la personne signant le message, ainsi que du contenu du message à signer. Une signature électronique doit être vérifiable : il doit être possible pour une tierce personne de vérifier la validité de la signature, sans que la connaissance de 15 la clé secrète de la personne signant le message ne soit requise.

Il existe deux types de schéma de signature électronique :

20 - Schémas de signature électronique nécessitant le message original pour la vérification de la signature.

- Schémas de signature électronique avec reconstitution du message. Le message original est 25 obtenu d'après la signature elle-même. Le message original n'étant pas nécessaire pour vérifier la signature, la taille totale de la signature est plus courte.

30 Il existe de nombreux procédés de signature électronique. Les plus connus sont :

- Schéma de signature RSA : c'est le schéma de signature électronique le plus largement utilisé. Sa sécurité est basée sur la difficulté de la factorisation de grands nombres ;

5

- Schéma de signature Rabin. Sa sécurité est aussi basée sur la difficulté de la factorisation de grands nombres ;

10 - Schéma de signature de type El-Gamal. Sa sécurité est basée sur la difficulté du problème du logarithme discret. Le problème du logarithme discret consiste à déterminer, s'il existe, un entier  $x$  tel que  $y=g^x$  avec  $y$  et  $g$  deux éléments d'un ensemble  $E$  possédant une structure de groupe ;

15 - Schéma de signature Schnorr. Il s'agit d'une variante du schéma de signature de type El-Gamal.

20 Il existe une autre variante du schéma de signature de type El-Gamal permettant la reconstitution totale du message, appelée schéma de signature Nyberg et Rueppel. Ce schéma est décrit dans l'article " A new signature scheme based on the DSA, giving message recovery " paru dans " Proceedings of the first ACM conference on communications and computer security, 1993, 58-61 ". Une variante de schéma à base de courbe elliptique est décrite dans le document " IEEE P1363 draft. Standard specifications 25 for public key cryptography. August 1998 ". Cette variante utilise une fonction de redondance  $R$ , une courbe elliptique formant une structure de groupe dont l'élément zéro est noté  $O$  et un point  $G$  de la courbe, lequel point  $G$  est générateur d'un sous-groupe d'ordre

un nombre premier  $r$ . La clé privée est un entier positif  $s$  inférieur à  $r$  et la clé publique est le point  $W=s.G$ , la notation  $s.G$  désignant la somme, au sens de l'addition de la courbe elliptique, de  $s$  points pris égaux à  $G$ . Le procédé de génération de la signature d'un message  $m$  comporte les cinq étapes suivantes :

- 1) Générer un nombre aléatoire  $u$  compris entre 0 et  $r-1$  et calculer  $V=u.G$  ;
- 2) Calculer l'entier  $f=R(m)$  ;
- 3) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f$  modulo  $r$  ; retourner à l'étape 1) si  $c=0$  ;
- 4) Calculer  $d=u-s*c$  modulo  $r$  ;
- 15 5) La signature est la paire d'entiers  $(c,d)$ .

Le procédé de vérification de la signature comporte les quatre étapes suivantes :

- 20 1) Si  $c$  n'appartient pas à l'intervalle  $[1,r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[0,r-1]$ , la signature n'est pas valide ;
- 2) Calculer le point  $P=d.G+c.W$ ; si  $P=0$ , la signature n'est pas valide ;
- 25 3) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f=c-i$  modulo  $r$  ;
- 4) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f=R(m)$  ; si oui, la signature du message  $m$  est valide ; sinon, la signature n'est pas valide.

30

Le premier procédé de l'invention consiste en une autre variante d'un schéma de signature de type El-Gamal. Cette variante permet la reconstitution totale du message. La variante est décrite dans le cadre de

l'utilisation de courbes elliptiques. Il est cependant possible d'utiliser cette variante dans tout ensemble possédant une structure de groupe pour lequel le problème du logarithme discret est difficile, par exemple le groupe multiplicatif des entiers modulo un nombre premier ou le sous-groupe multiplicatif d'ordre un grand nombre premier  $r$  des entiers modulo un nombre premier  $p$  avec  $r$  divisant  $p-1$ . Cette variante utilise une fonction de redondance  $R$ , une courbe elliptique formant une structure de groupe, dont l'élément zéro est noté  $O$  et un point  $G$  de la courbe, lequel point  $G$  est générateur d'un sous-groupe d'ordre un nombre premier  $r$ . La clé privée est un entier positif  $s$  inférieur à  $r$  et la clé publique est le point  $W=s.G$ . Cette variante utilise une constante entière  $k$  non nulle. Le procédé de génération de la signature comporte les quatre étapes suivantes :

- 1) Générer un nombre aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$  ;
- 2) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f$  modulo  $r$  ; si  $c=0$ , retourner à l'étape 1) ;
- 3) Calculer l'entier  $d=u^{-1}*(k+s*c)$  modulo  $r$  ; si  $d=0$ , retourner à l'étape 1) ;
- 4) La signature est la paire d'entiers  $(c,d)$ .

Le procédé correspondant de vérification de la signature comporte les six étapes suivantes :

- 1) Si  $c$  n'appartient pas à l'intervalle  $[1,r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1,r-1]$ , la signature n'est pas valide ;
- 2) Calculer les entiers  $h= d^{-1}$  modulo  $r$ ,  $h_1=k*h$  modulo  $r$  et  $h_2=c*h$  modulo  $r$  ;

3) Calculer le point  $P = h_1G + h_2W$ ; si  $P=O$ , la signature n'est pas valide;

4) Associer au point  $P$  un entier  $i$ ;

5) Calculer l'entier  $f=c-i$  modulo  $r$ ;

6) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f=R(m)$ ; si oui, la signature du message  $m$  est valide; sinon, la signature n'est pas valide.

Le procédé précédemment décrit permet donc d'obtenir un schéma de signature électronique dont la sécurité est basée sur la difficulté du problème du logarithme discret et permettant la reconstitution totale du message.

L'invention comprend également un second procédé de signature électronique permettant la reconstitution partielle du message. Le schéma de signature décrit précédemment permet la reconstitution totale du message. Cependant, la taille totale du message à signer est limitée par la taille des arguments de la fonction de redondance  $R$ . Le second procédé de l'invention permet de signer un message d'une taille quelconque. Le message  $m$  à signer est divisé en 2 parties: la première partie  $m_1$  de taille constante est reconstituée à partir de la signature, la deuxième partie  $m_2$  est transmise avec la signature du message. La taille totale de la signature et du message à transmettre est donc diminuée de la taille de la partie  $m_1$ . Le schéma de signature est décrit dans le cadre de l'utilisation de courbes elliptiques. Il est cependant possible d'utiliser ce schéma dans tout ensemble possédant une structure de groupe pour lequel le problème du logarithme discret est difficile, par exemple le groupe multiplicatif des entiers modulo un nombre premier ou le sous-groupe multiplicatif d'ordre

un grand nombre premier  $r$  des entiers modulo un nombre premier  $p$  avec  $r$  divisant  $p-1$ . Le schéma de signature utilise une fonction de redondance  $R$ , une courbe elliptique formant une structure de groupe dont l'élément zéro est noté  $O$  et un point  $G$  de la courbe, lequel point  $G$  est générateur d'un sous-groupe d'ordre un nombre premier  $r$ . La clé privée est un entier positif  $s$  inférieur à  $r$  et la clé publique est le point  $W=s.G$ . Le procédé de génération de la signature d'un message  $m$  constitué des messages  $m_1$  et  $m_2$  comporte les six étapes suivantes :

- 1) Générer un entier aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$  ;
- 2) Calculer  $f_1=R(m_1)$  ;
- 3) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f_1$  modulo  $r$  ; si  $c=0$ , retourner à l'étape 1 ;
- 4) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage ;
- 5) Calculer l'entier  $d=u^{-1}*(f_2+s*c)$  modulo  $r$  ; si  $d=0$ , retourner à l'étape 1 ;
- 6) La signature est le couple d'entiers  $(c,d)$ .

Le procédé de vérification de la signature prend en entrée une paire d'entiers  $(c,d)$  et le message partiel  $m_2$  et comprend les sept étapes suivantes :

- 1) Si  $c$  n'appartient pas à l'intervalle  $[1,r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1,r-1]$ , la signature n'est pas valide ;
- 2) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage ;
- 3) Calculer les entiers  $h=d^{-1}$  modulo  $r$ ,  $h_1=f_2*h$  modulo  $r$  et  $h_2=c*h$  modulo  $r$  ;

- 4) Calculer le point  $P = h_1G + h_2W$  ; si  $P=0$ , la signature n'est pas valide ;
- 5) Associer au point  $P$  l'entier  $i$  ;
- 6) Calculer l'entier  $f_1 = c - i$  modulo  $r$  ;
- 5 7) Obtenir le message  $m_1$  à partir de  $f_1$  et vérifier que  $f_1 = R(m_1)$  ; si oui, la signature du message  $m$  est valide ; sinon, la signature n'est pas valide.

Le procédé précédemment décrit permet donc d'obtenir un schéma de signature électronique dont la sécurité est basée sur la difficulté du logarithme discret et permettant la reconstitution partielle du message. L'intérêt d'un tel schéma est de diminuer la taille totale de la signature et du message à transmettre sans toutefois imposer de contrainte de taille à ce message.

L'invention consiste également en deux techniques générales permettant de minimiser la taille totale de la signature et du message à transmettre. La première technique consiste à inclure une partie du message à l'intérieur de la signature en choisissant convenablement les données aléatoires utilisées lors de la génération de la signature. La deuxième technique consiste à supprimer une partie des octets représentant la signature, la reconstitution complète de la signature s'effectuant durant la phase de vérification.

Le troisième procédé de l'invention consiste en une amélioration du schéma de signature de Nyberg-Rueppel rappelé précédemment, et consiste à inclure une partie du message de taille  $t$  octets dans l'entier  $d$  défini précédemment,  $t$  étant un entier petit. Dans ce procédé, les  $t$  octets de poids faible de l'entier  $d$  contiennent  $t$  octets du message. Le troisième procédé

de l'invention permet donc d'augmenter de  $t$  octets la taille du message à signer par rapport au schéma de signature de Nyberg-Rueppel décrit précédemment. Le troisième procédé utilise une fonction de redondance  $R$ , une courbe elliptique formant une structure de groupe dont l'élément zéro est noté  $O$  et un point  $G$  de la courbe, lequel point  $G$  est générateur d'un sous-groupe d'ordre un nombre premier  $r$ . La clé privée est un entier positif  $s$  inférieur à  $r$  et la clé publique est le point  $W=s.G$ . Le procédé de génération de la signature d'un message  $m$  comporte les cinq étapes suivantes :

- 1) Enlever les  $t$  octets de poids faible du message  $m$  et mémoriser le résultat dans  $m'$  ; calculer  $f=R(m')$  ;
- 2) Générer un nombre aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$  ;
- 3) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f$  modulo  $r$  ; retourner à l'étape 1) si  $c=0$ .
- 4) Calculer l'entier  $d=u-s*c$  modulo  $r$  ; si  $d$  n'est pas égal à  $m$  modulo  $2^t$  retourner à l'étape 2) ;
- 5) La signature est le couple d'entiers  $(c, d)$ .

Le procédé de vérification de la signature comporte les cinq étapes suivantes :

- 1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide ;
- 2) Calculer le point  $P=d.G+c.W$ ; si  $P=O$ , la signature n'est pas valide ;
- 3) Associer au point  $P$  l'entier  $i$  ;
- 4) Calculer l'entier  $f=c-i$  modulo  $r$  ;

5) Obtenir le message  $m'$  à partir de  $f$  et vérifier que  $f=R(m')$  ; si ce n'est pas le cas, la signature n'est pas valide ; si c'est le cas, la signature est valide et le message  $m$  est la concaténation au message 5  $m'$  des  $t$  octets de poids faible de l'entier  $d$ .

Il est possible d'effectuer un pré-traitement des données permettant d'accélérer la génération des signatures selon le schéma de signature décrit 10 précédemment. Le procédé de pré-traitement prend en entrée la clé "secrète  $s$ " et consiste à mettre en mémoire dans une table un grand nombre de valeurs  $(i, x_u)$  avec  $x_u = u - s * i$  modulo  $r$  et  $i$  étant l'entier associé au point  $V = u.G$ , de telle sorte que ces valeurs 15 puissent être accédées par le reste de  $x_u$  modulo  $2^{8t}$ . Le procédé de génération de signature avec pré-traitement des données utilise une fonction de redondance  $R$ , une courbe elliptique formant une structure de groupe dont l'élément zéro est noté  $O$  et 20 un point  $G$  de la courbe, lequel point  $G$  est générateur d'un sous-groupe d'ordre un nombre premier  $r$ . La clé privée est un entier positif  $s$  inférieur à  $r$  et la clé publique est le point  $W = s.G$ .

Le procédé de génération de signature avec pré-traitement des données comporte les huit étapes suivantes :

- 1) Enlever les  $t$  octets de poids faible du message  $m$  et mémoriser le résultat dans le message  $m'$  ; 30 calculer  $f = R(m')$ . Les  $t$  octets de poids faible du message  $m$  sont mémorisés dans l'entier  $\delta$  ;  
2) Calculer l'entier  $y = s * f$  modulo  $r$  et l'entier  $\lambda = y$  modulo  $2^{8t}$  ;

3) Si  $y < r/2$ , exécuter d'abord l'étape 4 et ensuite l'étape 5 ; sinon exécuter d'abord l'étape 5 et ensuite l'étape 4 ;

4) Accéder aux éléments de la table dont le reste modulo  $2^{8t}$  est  $\lambda+\delta$  modulo  $2^{8t}$  et sélectionner un élément tel que  $x_u$  est supérieur ou égal à  $y$  ; si un tel élément existe, il est supprimé de la table et le procédé passe à l'étape 6) ;

5) Accéder aux éléments de la table dont le reste modulo  $2^{8t}$  est  $\lambda+\delta+r$  modulo  $2^{8t}$  et sélectionner un élément tel que  $x_u$  est inférieur à  $y$  ; si un tel élément existe, il est supprimé de la table et le procédé passe à l'étape 6) ;

6) Calculer l'entier  $d = x_u - y$  modulo  $r$  ;

15 7) Obtenir l'entier  $i$  associé à  $x_u$  et calculer  $c = i + f$  modulo  $r$  ;

8) La signature est le couple d'entiers  $(c, d)$ .

Le quatrième procédé de l'invention consiste en une amélioration du schéma de signature à base de logarithme discret avec reconstitution partielle du message décrit précédemment. Le quatrième procédé de l'invention consiste à inclure une partie du message de taille  $t$  octets dans l'entier  $d$  défini précédemment,  $t$  étant un entier petit. Dans ce procédé, les  $t$  octets de poids faible de l'entier  $d$  contiennent  $t$  octets du message. Le quatrième procédé de l'invention permet donc de diminuer de  $t$  octets la taille totale de la signature et du message à transmettre. Le schéma de signature utilise une fonction de redondance  $R$ , une courbe elliptique formant une structure de groupe dont l'élément zéro est noté  $O$  et un point  $G$  de la courbe, lequel point  $G$  est générateur d'un sous-groupe d'ordre un nombre

premier  $r$ . La clé privée est un entier positif  $s$  inférieur à  $r$  et la clé publique est le point  $W=s.G$ . Le procédé de génération de la signature d'un message  $m$  constitué des messages  $m_1$  et  $m_2$  comporte les six 5 étapes suivantes:

1) Générer un entier aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u?G$  ;

2) Calculer  $f_1=R(m_1)$  ;

10 3) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f_1$  modulo  $r$  ; si  $c=0$ , retourner à l'étape 1 ;

4) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage ;

15 5) Calculer l'entier  $d=u^{-1}*(f_2+s*c)$  modulo  $r$  ; si  $d=0$  ou si  $d$  n'est pas égal à  $m_2$  modulo  $2^{8t}$ , retourner à l'étape 1 ;

6) La signature est le couple d'entiers  $(c,d)$  et le message à transmettre est  $m'_2$ , consistant en  $m_2$  privé de ses  $t$  octets de poids faible.

20

Le procédé de vérification de la signature prend en entrée une paire d'entiers  $(c,d)$  et le message partiel  $m'_2$ , et comprend les huit étapes suivantes :

25 1) Si  $c$  n'appartient pas à l'intervalle  $[1,r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1,r-1]$ , la signature n'est pas valide ;

2) Compléter  $m'_2$  en  $m_2$  en lui ajoutant les  $t$  octets de poids faible de  $d$  ;

30 3) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage ;

4) Calculer les entiers  $h=d^{-1}$  modulo  $r$ ,  $h_1=f_2*h$  modulo  $r$  et  $h_2=c*h$  modulo  $r$  ;

5) Calculer le point  $P = h_1G + h_2W$  ; si  $P=O$ , la signature n'est pas valide ;

6) Associer au point  $P$  l'entier  $i$  ;

7) Calculer l'entier  $f_1 = c - i$  modulo  $r$  ;

5 8) Obtenir le message  $m_1$  à partir de  $f_1$  et vérifier que  $f_1 = R(m_1)$  ; si oui, la signature du message  $m$  est valide ; sinon, la signature n'est pas valide ;

10 Le cinquième procédé de l'invention consiste à supprimer  $t$  octets de la chaîne d'octets représentant l'entier  $d$  lorsque la signature est le couple d'entiers  $(c, d)$ . Ce procédé s'applique au schéma de signature de Nyberg et Rueppel ainsi qu'au schéma de signature avec reconstitution partielle du message 15 précédemment décrit. Le procédé modifié de génération de signature comporte les deux étapes suivantes :

20 1) Générer la signature du message  $m$  en utilisant le schéma de signature de Nyberg et Rueppel ou le schéma de signature avec reconstitution partielle du message précédemment décrit, pour obtenir le couple 25 d'entiers  $(c, d)$  ;

2) Calculer  $d'$ , quotient entier de la division de l'entier  $d$  par  $2^{8t}$ . La signature est le couple d'entiers  $(c, d')$ .

Le procédé modifié de vérification de signature prend en entrée un couple  $(c, d')$  et un message  $m_2$  et comporte les 2 étapes suivantes dans le cas de 30 l'utilisation du schéma de signature avec reconstitution partielle du message précédemment décrit :

1) Pour  $i$  allant de 0 à  $2^{8t}-1$ , calculer l'entier  $d=d'*2^{8t}+i$  et exécuter le procédé de vérification de signature avec reconstitution partielle du message précédemment décrit, la signature à vérifier étant (c, d) ; si le procédé de vérification de signature reconnaît la signature (c, d) comme valide, la signature est valide, et le procédé est terminé ;

5 2) Si l'étape 1) n'a pas abouti, la signature n'est pas valide.

10

Dans le cas de l'utilisation du schéma de signature de Nyberg-Rueppel, le procédé de vérification de signature prend en entrée un couple (c, d') et comporte les cinq étapes suivantes :

15

1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide ;

2) Calculer le point  $P=d'*2^{8t}.G+c.W$  ;

20 3) Pour  $j$  allant de 0 à  $2^{8t}-1$ , exécuter les étapes suivantes :

3)a) Si  $P=O$ , exécuter l'étape 3)d) ;

3)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f=c-i$  modulo  $r$  ;

25 3)c) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f=R(m)$  ; si oui, exécuter l'étape 5) ;

3)d) Remplacer  $P$  par  $P+G$  ;

4) La signature n'est pas valide et le procédé est terminé ;

30 5) Si l'entier  $d=d'*2^{8t}+j$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide ; sinon la signature est valide et le procédé est terminé.

Le sixième procédé de l'invention consiste en une modification du schéma de signature de Nyberg et Rueppel permettant d'augmenter de  $t$  octets la taille des messages à signer,  $t$  étant une variable entière.

5 Le sixième procédé utilise une fonction de redondance  $R$ , une courbe elliptique formant une structure de groupe dont l'élément zéro est noté  $O$  et un point  $G$  de la courbe, lequel point  $G$  est générateur d'un sous-groupe d'ordre un nombre premier  $r$ . La clé privée est  
10 un entier positif  $s$  inférieur à  $r$  et la clé publique est le point  $W=s.G$ . Le procédé de génération de la signature d'un message  $m$  comporte les cinq étapes suivantes :

15 1) Générer un nombre aléatoire  $u$  et calculer  $V=u.G$  ;

2) Obtenir le message  $m'$  en enlevant au message  $m$  les  $t$  octets de poids faible et calculer  $f=R(m')$  ;

20 3) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f$  modulo  $r$  ; retourner à l'étape 1) si  $c=0$  ou si  $i$  n'est pas égal à  $m$  modulo  $2^{8t}$  ;

4) Calculer  $d=u-s*c$  modulo  $r$  ;

5) La signature est la paire d'entiers  $(c,d)$ .

25 Le procédé de vérification de la signature comporte les quatre étapes suivantes :

1) Si  $c$  n'appartient pas à l'intervalle  $[1,r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[0,r-1]$ , la  
30 signature n'est pas valide ;

2) Calculer le point  $P=d.G+c.W$ ; si  $P=O$ , la signature n'est pas valide ;

3) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f=c-i$  modulo  $r$  ;

4) Retrouver le message  $m'$  à partir de  $f$  et vérifier que  $f=R(m')$  ; si oui, retrouver le message  $m$  en concaténant au message  $m'$  les  $t$  octets de poids faible de  $i$ . La signature du message  $m$  est alors valide ; sinon, la signature n'est pas valide.

Le septième procédé de l'invention consiste en une modification du schéma de signature avec reconstitution partielle du message précédemment décrit permettant d'augmenter de  $t$  octets la taille du message  $m_1$  reconstruit à partir de la signature,  $t$  étant une variable entière. Le septième procédé utilise une fonction de redondance  $R$ , une courbe elliptique formant une structure de groupe dont l'élément zéro est noté  $O$  et un point  $G$  de la courbe, lequel point  $G$  est générateur d'un sous-groupe d'ordre un nombre premier  $r$ . La clé privée est un entier positif  $s$  inférieur à  $r$  et la clé publique est le point  $W=s.G$ . Le procédé de génération de la signature d'un message  $m$ , constitué de deux messages  $m_1$  et  $m_2$ , comporte les six étapes suivantes :

- 1) Générer un entier aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$  ;
- 2) Obtenir  $m'_1$  en enlevant au message  $m_1$  les  $t$  octets de poids faible. Calculer  $f_1=R(m'_1)$  ;
- 3) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f_1$  modulo  $r$  ; si  $c=0$  ou si  $i$  n'est pas égal à  $m_1$  modulo  $2^{8t}$ , retourner à l'étape 1 ;
- 4) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage ;
- 5) Calculer l'entier  $d=u^{-1}*(f_2+s*c)$  modulo  $r$  ; si  $d=0$ , retourner à l'étape 1 ;
- 6) La signature est le couple d'entiers  $(c,d)$ .

Le procédé de vérification de la signature prend en entrée une paire d'entiers  $(c, d)$  et le message partiel  $m_2$  et comprend les sept étapes suivantes :

5

1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide ;

10 2) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage ;

3) Calculer les entiers  $h= d^{-1}$  modulo  $r$ ,  $h_1= f_2 \cdot h$  modulo  $r$  et  $h_2=c \cdot h$  modulo  $r$  ;

4) Calculer le point  $P= h_1G+ h_2W$ ; si  $P=O$ , la signature n'est pas valide.

15

5) Associer au point  $P$  l'entier  $i$  ;

6) Calculer l'entier  $f_1=c-i$  modulo  $r$  ;

20 7) Obtenir le message  $m'_1$  à partir de  $f_1$  et vérifier que  $f_1=R(m'_1)$  ; si oui, obtenir  $m_1$  en concaténant au message  $m'_1$  les  $t$  octets de poids faible de l'entier  $i$ . La signature du message  $m$  est alors valide ; sinon, la signature n'est pas valide.

Il est possible pour les sixièmes et septièmes procédés de diminuer les temps de calcul en effectuant des pré-traitements. Ces pré-traitements consistent à mettre en mémoire dans une table des couples d'entiers  $(u, i)$  tels que définis précédemment de telle sorte que ces entiers soient accessibles par la valeur de  $i$  modulo  $2^{8t}$ .

30 Le huitième procédé de l'invention consiste en une modification du schéma de signature de Nyberg et Rueppel consistant à enlever  $t$  octets à l'entier  $c$  précédemment défini,  $t$  étant une variable entière. Le

procédé de génération de signature comporte les deux étapes suivantes :

5 1) Générer la signature du message  $m$  en utilisant le schéma de signature de Nyberg-Rueppel pour obtenir le couple d'entiers  $(c, d)$  ;

10 2) Calculer  $c'$ , quotient entier de la division de l'entier  $c$  par  $2^{8t}$ . La signature est le couple d'entiers  $(c', d)$ .

Le procédé de vérification de signature prend en entrée le couple d'entiers  $(c', d)$  et comporte les cinq étapes suivantes :

15 1) Si  $d$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide ;

2) Calculer le point  $P=d.G+c' * 2^{8t}.W$  ;

3) Pour  $j$  allant de 0 à  $2^{8t}-1$ , exécuter les étapes suivantes :

20 3)a) Si  $P=O$ , exécuter l'étape 3)d) ;

3)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f=c-i$  modulo  $r$  ;

3)c) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f=R(m)$  ; si oui, exécuter l'étape

25 5) ;

3)d) Remplacer  $P$  par  $P+W$  ;

4) La signature n'est pas valide et le procédé est terminé ;

30 5) Si l'entier  $c=c'*2^{8t}+j$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide ; sinon la signature est valide et le procédé est terminé.

Le neuvième procédé de l'invention est une modification du schéma de signature avec reconstitution partielle du message défini précédemment, qui consiste à enlever  $t$  octets de 5 l'entier  $c$  défini précédemment,  $t$  étant une variable entière. Le procédé de génération de signature comprend les deux étapes suivantes :

1) Générer la signature du message  $m$ , constitué de 10 deux messages  $m_1$  et  $m_2$ , en utilisant le schéma de signature avec reconstitution partielle du message pour obtenir le couple d'entiers  $(c, d)$  ;

2) Calculer  $c'$ , quotient entier de la division de l'entier  $c$  par  $2^{8t}$ . La signature est le couple 15 d'entiers  $(c', d)$ .

Le procédé de vérification de signature prend en entrée un couple d'entiers  $(c', d)$  et un message  $m_2$  et comprend les huit étapes suivantes :

20 1) Si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide ;

2) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage ;

25 3) Calculer les entiers  $h = d^{-1}$  modulo  $r$ ,  $h_1 = f_2 * h$  modulo  $r$  et  $h_2 = c' * 2^{8t} + h$  modulo  $r$  ;

4) Calculer le point  $P = h_1 \cdot G + h_2 \cdot W$  ;

5) Calculer le point  $Z = h \cdot W$  ;

30 6) Pour  $j$  allant de 0 à  $2^{8t}-1$ , exécuter les étapes suivantes :

6)a) Si  $P=O$ , exécuter l'étape 6)d) ;

6)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f_1 = c - i$  modulo  $r$  ;

6)c) Retrouver le message  $m_1$  à partir de  $f_1$  et vérifier que  $f_1=R(m_1)$  ; si oui, exécuter l'étape 8) ;

6)d) Remplacer  $P$  par  $P+Z$  ;

5 7) La signature n'est pas valide et le procédé est terminé ;

8) Si l'entier  $c=c'*2^{8t}+j$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide ; sinon la signature est valide et le procédé est 10 terminé.

Le dixième procédé de l'invention consiste en une modification du schéma de signature avec reconstitution partielle du message précédemment 15 décrit, qui consiste à remplacer la signature  $(c, d)$  par la signature  $(h_2, d)$  avec  $h_2=c*d^{-1}$  modulo  $r$ . L'avantage de ce dixième procédé est de permettre une réduction du temps de calcul lorsque ce procédé est appliqué à l'un quelconque des procédés définis 20 précédemment.

Le onzième procédé de l'invention consiste en une amélioration du schéma de signature de Nyberg-Rueppel rappelé précédemment, et consiste à inclure une partie du message de taille  $t$  octets dans l'entier  $d$  défini 25 précédemment,  $t$  étant un entier petit, ainsi qu'à utiliser une autre fonction de redondance. Dans ce procédé, les  $t$  octets de poids faible de l'entier  $d$  contiennent  $t$  octets du message. Le onzième procédé utilise une courbe elliptique formant une structure de 30 groupe dont l'élément zéro est noté  $O$  et un point  $G$  de la courbe, lequel point  $G$  est générateur d'un sous-groupe d'ordre un nombre premier  $r$ . La clé privée est un entier positif  $s$  inférieur à  $r$  et la clé publique est le point  $W=s.G$ . Le procédé de génération de la

signature d'un message  $m$  utilise les paramètres entiers  $t$ ,  $a$ , et  $k$  et comporte les sept étapes suivantes :

- 5        1) Calculer  $h=H(m)$ ,  $H$  étant une fonction de hachage ;
- 2) Enlever les  $t$  octets de poids faible et les  $k$  octets de poids fort du message  $m$  et mémoriser le résultat dans  $m'$  ;
- 10      3) Mémoriser dans  $f$  le résultat de la concaténation à  $m'$  des  $a$  octêts de poids fort de  $h$  ;
- 4) Générer un nombre aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$  ;
- 5) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f \text{ modulo } r$  ; retourner à l'étape 4) si  $c=0$  ;
- 6) Calculer l'entier  $d=u-s*c \text{ modulo } r$  ; si  $d$  n'est pas égal à  $m$  modulo  $2^{8t}$  retourner à l'étape 4) ;
- 7) La signature est le couple d'entiers  $(c,d)$ .

20      Le procédé de vérification de la signature comporte les sept étapes suivantes :

- 1) Si  $c$  n'appartient pas à l'intervalle  $[1,r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[0,r-1]$ , la signature n'est pas valide ;
- 2) Calculer le point  $P=d.G+c.W$ ; si  $P=0$ , la signature n'est pas valide ;
- 3) Associer au point  $P$  l'entier  $i$  ;
- 4) Calculer l'entier  $f=c-i \text{ modulo } r$  ;
- 30      5) Concaténer au message  $m'$  obtenu à partir de  $f$  en enlevant les  $a$  octêts de poids faible les  $t$  octets de poids faible de  $d$  ;
- 6) Pour  $b$  allant de 0 à  $2^{8k}-1$  répéter l'étape suivante :

6) a) Concaténer à  $b$  le message  $m'$  pour obtenir  $m$  et calculer  $h = H(m)$  ; Vérifier que les  $a$  octets de poids fort de  $h$  et les  $a$  octets de poids faible de  $f$  sont identiques ; si oui, la signature du message  $m$  est valide et le procédé est terminé ;  
7) La signature n'est pas valide.

5 message m est valide et le procédé est terminé ;

7) La signature n'est pas valide.

Les procédés décrits permettent donc de réduire de façon significative la taille totale de la signature et du message à transmettre. Lorsque la place en mémoire est limitée, il est ainsi possible de stocker un plus grand nombre de signatures. En outre, il est également possible de réaliser une transmission plus rapide des signatures. Ces procédés sont particulièrement destinées à être mises en place dans des dispositifs portables, par exemple de type carte à puce.

**REVENDICATIONS**

1- Procédé de signature électronique comprenant un procédé de génération et un procédé de vérification permettant une reconstitution totale du message, ledit procédé utilisant une fonction de redondance  $R$ , un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté  $O$  et de générateur le point  $G$ , la clé privée étant un entier positif inférieur à  $r$ , la clé publique étant le point  $W=s.G$ , ledit procédé utilisant une constante entière  $k$  non nulle, caractérisé en ce que le procédé de génération de signature comporte les 4 étapes suivantes :

- 1) Générer un nombre aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$  ;
- 2) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f$  modulo  $r$  ; si  $c=0$ , retourner à l'étape 1) ;
- 3) Calculer l'entier  $d=u^{-1}*(k+s*c)$  modulo  $r$  ; si  $d=0$ , retourner à l'étape 1) ;
- 4) La signature est la paire d'entiers  $(c,d)$  ;

et en ce que le procédé de vérification de la signature comporte les 6 étapes suivantes :

- 1) Si  $c$  n'appartient pas à l'intervalle  $[1,r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1,r-1]$ , la signature n'est pas valide ;
- 2) Calculer les entiers  $h=d^{-1}$  modulo  $r$ ,  $h_1=k*h$  modulo  $r$  et  $h_2=c*h$  modulo  $r$  ;
- 3) Calculer le point  $P=h_1G+h_2W$  ; si  $P=O$ , la signature n'est pas valide ;
- 4) Associer au point  $P$  un entier  $i$  ;
- 5) Calculer l'entier  $f=c-i$  modulo  $r$  ;

6) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f=R(m)$  ; si oui, la signature du message  $m$  est valide ; sinon, la signature n'est pas valide.

5 2- Procédé de signature électronique comprenant un procédé de génération et un procédé de vérification de signature permettant une reconstitution partielle du message, le message  $m$  à signer étant divisé en deux parties, la première partie  $m_1$  de taille constante  
10 étant reconstituée à partir de la signature, la deuxième partie  $m_2$  étant transmise avec la signature du message, ledit procédé utilisant une fonction de redondance  $R$ , un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro  
15 noté 0 et de générateur le point  $G$ , la clé privée étant un entier positif inférieur à  $r$  et la clé publique étant le point  $W=s.G$ , caractérisé en ce que le procédé de génération de la signature d'un message  $m$  constitué des messages  $m_1$  et  $m_2$  comporte les 6 étapes  
20 suivantes :

1) Générer un entier aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$  ;

2) Calculer  $f_1=R(m_1)$  ;

25 3) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f_1$  modulo  $r$ ; si  $c=0$ , retourner à l'étape 1 ;

4) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage ;

30 5) Calculer l'entier  $d=u^{-1}*(f_2+s*c)$  modulo  $r$  ; si  $d=0$ , retourner à l'étape 1 ;

6) La signature est le couple d'entiers  $(c,d)$  ;

et en ce que le procédé de vérification de la signature prend en entrée une paire d'entiers  $(c, d)$  et le message partiel  $m_2$  et comprend les 7 étapes suivantes :

5           1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide ;

10          2) Calculer  $f_2 = H(m_2)$ , où  $H$  est une fonction de hachage ;

             3) Calculer les entiers  $h = d^{-1}$  modulo  $r$ ,  $h_1 = f_2 * h$  modulo  $r$  et  $h_2 = c * h$  modulo  $r$  ;

             4) Calculer le point  $P = h_1 G + h_2 W$ ; si  $P=O$ , la signature n'est pas valide ;

15          5) Associer au point  $P$  l'entier  $i$  ;

             6) Calculer l'entier  $f_1 = c - i$  modulo  $r$  ;

             7) Obtenir le message  $m_1$  à partir de  $f_1$  et vérifier que  $f_1 = R(m_1)$  ; si oui, la signature du message  $m$  est valide ; sinon, la signature n'est pas valide.

20          3- Procédé de signature électronique comprenant un procédé de génération et un procédé de vérification de signature caractérisé en ce qu'il consiste à inclure une partie du message à l'intérieur de la signature en 25 choisissant convenablement les données aléatoires utilisées lors de la génération de la signature.

             4- Procédé de signature électronique comprenant un procédé de génération et un procédé de vérification de 30 signature caractérisé en ce qu'il consiste à supprimer une partie des octets représentant la signature, la

reconstitution complète de la signature s'effectuant durant la phase de vérification.

5- Procédé d'amélioration du schéma de signature de Nyberg-Rueppel selon la revendication 3 comprenant un procédé de génération et un procédé de vérification et consistant à inclure une partie du message de taille t octets dans l'entier d, t étant un entier petit, la signature étant le couple d'entiers  $(c,d)$ , les t octets de poids faible de l'entier d contenant t octets du message, ledit procédé utilisant une fonction de redondance R, un ensemble possédant une structure de groupe d'ordre un nombre premier r, d'élément zéro noté 0 et de générateur le point G, la clé privée étant un entier positif s inférieur à r et la clé publique étant le point  $W=s.G$ , caractérisé en ce que le procédé de génération de la signature d'un message m comporte les 5 étapes suivantes :

- 20 1) Enlever les t octets de poids faible du message m et mémoriser le résultat dans  $m'$  ; calculer  $f=R(m')$  ;
  - 2) Générer un nombre aléatoire u compris entre 1 et  $r-1$  et calculer  $V=u.G$  ;
  - 25 3) Associer au point V un entier i et calculer  $c=i+f$  modulo r ; retourner à l'étape 1) si  $c=0$  ;
  - 4) Calculer l'entier  $d=u-s*c$  modulo r ; si d n'est pas égal à m modulo  $2^t$  retourner à l'étape 2) ;
  - 5) La signature est le couple d'entiers  $(c,d)$  ;
- 30 et en ce que le procédé de vérification de la signature comporte les 5 étapes suivantes :

1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide ;

5 2) Calculer le point  $P=d.G+c.W$  ; si  $P=O$ , la signature n'est pas valide ;

3) Associer au point  $P$  l'entier  $i$  ;

4) Calculer l'entier  $f=c-i$  modulo  $r$  ;

10 5) Obtenir le message  $m'$  à partir de  $f$  et vérifier que  $f=R(m')$  ; si ce n'est pas le cas, la signature n'est pas valide ; si c'est le cas, la signature est valide et le message  $m$  est la concaténation au message  $m'$  des  $t$  octets de poids faible de l'entier  $d$ .

15 6- Procédé de pré-traitement de la génération de signature selon la revendication 5 permettant d'accélérer la génération des signatures, ledit procédé comprenant une phase de pré-traitement et une phase de génération de la signature, ladite phase de pré-traitement prenant en entrée la clé secrète  $s$  et consistant à mettre en mémoire dans une table un grand nombre de valeurs  $(i, x_u)$  avec  $x_u=u-s*i$  modulo  $r$  et  $i$  étant l'entier associé au point  $V=u.G$ , de telle sorte que ces valeurs puissent être accédées par le reste de 25  $x_u$  modulo  $2^{8t}$ , ladite phase de génération de signature utilisant une fonction de redondance  $R$ , un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté  $O$  et de générateur le point  $G$ , la clé privée étant un entier positif  $s$  inférieur à  $r$  et la clé publique étant le point  $W=s.G$ , ladite phase de génération de la signature étant caractérisé par les 8 étapes suivantes :

- 1) Enlever les  $t$  octets de poids faible du message  $m$  et mémoriser le résultat dans  $m'$  ; calculer  $f=R(m')$  ; les  $t$  octets de poids faible du message  $m$  sont mémorisés dans l'entier  $\delta$ .  
5
- 2) Calculer l'entier  $y=s*f$  modulo  $r$  et l'entier  $\lambda=y$  modulo  $2^{8t}$  ;
- 3) Si  $y < r/2$ , exécuter d'abord l'étape 4 et ensuite l'étape 5, sinon exécuter d'abord l'étape 5 et ensuite  
10 l'étape 4 ;
- 4) Accéder aux éléments de la table dont le reste modulo  $2^{8t}$  est  $\lambda+\delta$  modulo  $2^{8t}$  et sélectionner un élément tel que  $x_u$  est supérieur ou égal à  $y$  ; si un tel élément existe, il est supprimé de la table et le  
15 procédé passe à l'étape 6) ;
- 5) Accéder aux éléments de la table dont le reste modulo  $2^{8t}$  est  $\lambda+\delta+r$  modulo  $2^{8t}$  et sélectionner un élément tel que  $x_u$  est inférieur à  $y$  ; si un tel élément existe, il est supprimé de la table et le  
20 procédé passe à l'étape 6) ;
- 6) Calculer l'entier  $d= x_u-y$  modulo  $r$  ;
- 7) Obtenir l'entier  $i$  associé à  $x_u$  et calculer  $c=i+f$  modulo  $r$  ;
- 8) La signature est le couple d'entiers  $(c,d)$ .

25

7- Procédé d'amélioration du schéma de signature avec reconstitution partielle du message selon la revendication 2, ledit procédé comprenant un procédé de génération de la signature et un procédé de  
30 vérification de la signature, ledit procédé consistant à inclure une partie du message de taille  $t$  octets

dans l'entier d défini précédemment, t étant un entier petit, les t octets de poids faible de l'entier d contenant t octets du message, ledit procédé utilisant une fonction de redondance R, un ensemble possédant 5 une structure de groupe d'ordre un nombre premier r, d'élément zéro noté 0 et de générateur le point G, la clé privée étant un entier positif inférieur à r et la clé publique étant le point  $W=s.G$ , caractérisé en ce que le procédé de génération de la signature d'un 10 message m constitué des messages  $m_1$  et  $m_2$  comporte les 6 étapes suivantes :

- 1) Générer un entier aléatoire u compris entre 1 et  $r-1$  et calculer  $V=u.G$  ;
- 15 2) Calculer  $f_1=R(m_1)$  ;
- 3) Associer au point V un entier i et calculer  $c=i+f_1$  modulo r ; si  $c=0$ , retourner à l'étape 1 ;
- 4) Calculer  $f_2=H(m_2)$ , où H est une fonction de hachage ;
- 20 5) Calculer l'entier  $d=u^{-1}*(f_2+s*c)$  modulo r ; si  $d=0$  ou si d n'est pas égal à  $m_2$  modulo  $2^{8t}$  retourner à l'étape 1) ;
- 6) La signature est le couple d'entiers (c,d) et le message à transmettre est  $m'_2$  consistant en  $m_2$  privé 25 de ses t octets de poids faible ;

et en ce que le procédé de vérification de la signature prend en entrée une paire d'entiers (c,d) et le message partiel  $m'_2$  et comprend les 8 étapes 30 suivantes :

1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide ;

2) Compléter  $m'_2$  en  $m_2$  en lui ajoutant les  $t$  octets de poids faible de  $d$  ;

3) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage ;

4) Calculer les entiers  $h = d^{-1}$  modulo  $r$ ,  $h_1 = f_2 * h$  modulo  $r$  et  $h_2 = c * h$  modulo  $r$  ;

10 5) Calculer le point  $P = h_1 G + h_2 W$  ; si  $P=O$ , la signature n'est pas valide ;

6) Associer au point  $P$  l'entier  $i$  ;

7) Calculer l'entier  $f_1=c-i$  modulo  $r$  ;

15 8) Obtenir le message  $m_1$  à partir de  $f_1$  et vérifier que  $f_1=R(m_1)$  ; si oui, la signature du message  $m$  est valide ; sinon, la signature n'est pas valide.

8- Procédé consistant à enlever  $t$  octets de la chaîne d'octets représentant l'entier  $d$  lorsque la signature est le couple d'entiers  $(c,d)$ , ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, ledit procédé s'appliquant au schéma de signature de Nyberg et Rueppel, caractérisé en ce que le procédé modifié de génération de signature comporte les 2 étapes suivantes :

30 1) Générer la signature du message  $m$  en utilisant le schéma de signature de Nyberg et Rueppel, pour obtenir le couple d'entiers  $(c,d)$  ;

2) Calculer  $d'$ , quotient entier de la division de l'entier  $d$  par  $2^{8t}$ ; la signature est le couple d'entiers  $(c,d')$ ;

5 et en ce que le procédé modifié de vérification de signature prend en entrée un couple  $(c,d')$  et comporte les 5 étapes suivantes :

1) Si  $c$  n'appartient pas à l'intervalle  $[1,r-1]$ ,  
10 la signature n'est pas valide ;  
2) Calculer le point  $P=d'*2^{8t}.G+c.W$  ;  
3) Pour  $j$  allant de 0 à  $2^{8t}-1$ , exécuter les étapes suivantes:

15       3)a) Si  $P=0$ , exécuter l'étape 3)d) ;  
          3)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f=c-i$  modulo  $r$  ;  
          3)c) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f=R(m)$ ; si oui, exécuter l'étape 5) ;  
          3)d) Remplacer  $P$  par  $P+G$  ;  
20       4) La signature n'est pas valide et le procédé est terminé ;  
          5) Si l'entier  $d=d'*2^{8t}+j$  n'appartient pas à l'intervalle  $[0,r-1]$ , la signature n'est pas valide ; sinon la signature est valide et le procédé est  
25 terminé.

9- Procédé consistant à enlever  $t$  octets de la chaîne d'octets représentant l'entier  $d$  lorsque la signature est le couple d'entiers  $(c,d)$ , ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, ledit procédé au schéma de signature avec reconstitution

partielle du message selon la revendication 2, caractérisé en ce que le procédé modifié de génération de signature comporte les 2 étapes suivantes :

5        1) Générer la signature du message  $m$  en utilisant le schéma de signature avec reconstitution partielle du message précédemment décrit, pour obtenir le couple d'entiers  $(c, d)$  ;

10      2) Calculer  $d'$ , quotient entier de la division de l'entier  $d$  par  $2^{8t}$  ; la signature est le couple d'entiers  $(c, d')$  ;

et en ce que le procédé modifié de vérification de signature prend en entrée un couple  $(c, d')$  et un message  $m_2$  et comporte les 2 étapes suivantes :

20      1) Pour  $i$  allant de 0 à  $2^{8t}-1$ , calculer l'entier  $d=d'*2^{8t}+i$  et exécuter le procédé de vérification de signature avec reconstitution partielle du message précédemment décrit, la signature à vérifier étant  $(c, d)$  ; si le procédé de vérification de signature reconnaît la signature  $(c, d)$  comme valide, la signature est valide, et le procédé est terminé ;

25      2) La signature n'est pas valide.

25

10- Procédé d'amélioration du schéma de Nyberg et Rueppel permettant d'augmenter de  $t$  octets la taille des messages à signer,  $t$  étant une variable entière, ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, ledit procédé utilisant une fonction de redondance  $R$ , un ensemble possédant une structure de

groupe d'ordre un nombre premier  $r$ , d'élément zéro noté  $O$  et de générateur le point  $G$ , la clé privée étant un entier positif  $s$  inférieur à  $r$  et la clé publique étant le point  $W=s.G$ , caractérisé en ce que  
5 le procédé de génération de la signature d'un message  $m$  comporte les 5 étapes suivantes:

- 1) Générer un nombre aléatoire  $u$  et calculer  $V=u.G$  ;
- 10 2) Obtenir le message  $m'$  en enlevant au message  $m$  les  $t$  octets de poids faible et calculer  $f=R(m')$  ;
- 3) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f$  modulo  $r$  ; retourner à l'étape 1) si  $c=0$  ou si  $i$  n'est pas égal à  $m$  modulo  $2^{8t}$  ;
- 15 4) Calculer  $d=u-s*c$  modulo  $r$  ;
- 5) La signature est la paire d'entiers  $(c,d)$  ;

et en ce que le procédé de vérification de la signature comporte les 4 étapes suivantes:

- 20 1) Si  $c$  n'appartient pas à l'intervalle  $[1,r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[0,r-1]$ , la signature n'est pas valide ;
- 2) Calculer le point  $P=d.G+c.W$ ; si  $P=O$ , la signature n'est pas valide ;
- 25 3) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f=c-i$  modulo  $r$  ;
- 30 4) Retrouver le message  $m'$  à partir de  $f$  et vérifier que  $f=R(m')$  ; si oui, retrouver le message  $m$  en concaténant au message  $m'$  les  $t$  octets de poids faible de  $i$  ; la signature du message  $m$  est alors valide ; sinon, la signature n'est pas valide.

11- Procédé d'amélioration du schéma de signature avec reconstitution partielle du message selon la revendication 2, ledit procédé comprenant un procédé 5 de génération de la signature et un procédé de vérification de la signature, ledit procédé permettant d'augmenter de  $t$  octets la taille du message  $m_1$  reconstitué à partir de la signature,  $t$  étant une variable entière, ledit procédé utilisant une fonction 10 de redondance  $R$ , un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté  $O$  et de générateur le point  $G$ , la clé privée étant un entier positif inférieur à  $r$  et la clé publique étant le point  $W=s.G$ , caractérisé en ce que 15 le procédé de génération de la signature d'un message  $m$  comporte les 6 étapes suivantes :

- 1) Générer un entier aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$  ;
  - 2) Obtenir  $m'_1$  en enlevant au message  $m_1$  les  $t$  octets de poids faible ; calculer  $f_1=R(m'_1)$  ;
  - 3) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f_1$  modulo  $r$  ; si  $c=0$  ou si  $i$  n'est pas égal à  $m_1$  modulo  $2^{8t}$  ; retourner à l'étape 1 ;
  - 4) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage ;
  - 5) Calculer l'entier  $d=u^{-1}*(f_2+s*c)$  modulo  $r$  ; si  $d=0$ , retourner à l'étape 1 ;
  - 6) La signature est le couple d'entiers  $(c,d)$  ;
- et en ce que le procédé de vérification de la signature prend en entrée une paire d'entiers  $(c,d)$  et

le message partiel  $m_2$  et comprend les 7 étapes suivantes:

1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou 5 si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide ;

2) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage ;

3) Calculer les entiers  $h = d^{-1}$  modulo  $r$ ,  $h_1 = f_2 * h$  10 modulo  $r$  et  $h_2 = c * h$  modulo  $r$  ;

4) Calculer le point  $P = h_1G + h_2W$ ; si  $P=O$ , la signature n'est pas valide ;

5) Associer au point  $P$  l'entier  $i$  ;

6) Calculer l'entier  $f_1 = c - i$  modulo  $r$  ;

15 7) Obtenir le message  $m'_1$  à partir de  $f_1$  et vérifier que  $f_1 = R(m'_1)$  ; si oui, obtenir  $m_1$  en concaténant au message  $m'_1$  les  $t$  octets de poids faible de l'entier  $i$  ; la signature du message  $m$  est alors valide ; sinon, la signature n'est pas valide.

20 '

12- Procédé de pré-traitement des calculs permettant d'augmenter les performances des procédés selon les revendications 10 et 11, caractérisé en ce qu'il consiste à mettre en mémoire dans une table des 25 couples d'entiers  $(u, i)$  de telle sorte que ces entiers soient accessibles par la valeur de  $i$  modulo  $2^{8t}$ ,  $t$  étant un paramètre entier.

13- Procédé d'amélioration du schéma de signature de 30 Nyberg et Rueppel consistant à enlever  $t$  octets à l'entier  $c$ ,  $t$  étant une variable entière, ledit procédé comprenant un procédé de génération de la

signature et un procédé de vérification de la signature, la signature étant constitué du couple d'entiers  $(c, d)$ , caractérisé en ce que le procédé de génération de signature comporte les 2 étapes suivantes:

1) Générer la signature du message  $m$  en utilisant le schéma de signature de Nyberg-Rueppel pour obtenir le couple d'entiers  $(c, d)$  ;

2) Calculer  $c'$ , quotient entier de la division de l'entier  $c$  par  $2^{8t}$  ; la signature est le couple d'entiers  $(c', d)$  ;

et en ce que le procédé de vérification de signature prend en entrée le couple d'entiers  $(c', d)$  et comporte les 5 étapes suivantes:

1) Si  $d$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide ;

2) Calculer le point  $P=d.G+c'*2^{8t}.W$  ;

3) Pour  $j$  allant de 0 à  $2^{8t}-1$  ; exécuter les étapes suivantes:

3)a) Si  $P=0$ , exécuter l'étape 3)d) ;

3)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f=c-i$  modulo  $r$  ;

3)c) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f=R(m)$  ; si oui, exécuter l'étape 5) ;

3)d) Remplacer  $P$  par  $P+W$  ;

4) La signature n'est pas valide et le procédé est terminé ;

5) Si l'entier  $c=c'*2^{8t}+j$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide, sinon la signature est valide et le procédé est terminé.

5

14- Procédé d'amélioration du schéma de signature avec reconstitution partielle du message selon la revendication 2 consistant à enlever  $t$  octets de l'entier  $c$  défini selon la revendication 2,  $t$  étant une variable entière, ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, caractérisé en ce que le procédé de génération de signature comprend les deux étapes suivantes :

15

- 1) Générer la signature du message  $m$  en utilisant le schéma de signature avec reconstitution partielle du message pour obtenir le couple d'entiers  $(c, d)$  ;
- 2) Calculer  $c'$ , quotient entier de la division de l'entier  $c$  par  $2^{8t}$  ; la signature est le couple d'entiers  $(c', d)$  ;

et en ce que le procédé de vérification de signature prend en entrée un couple d'entiers  $(c', d)$  et un message  $m_2$  et comprend les 8 étapes suivantes:

- 1) Si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide ;
- 2) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage ;
- 3) Calculer les entiers  $h= d^{-1}$  modulo  $r$ ,  $h_1= f_2 * h$  modulo  $r$  et  $h_2=c'*2^{8t}*h$  modulo  $r$  ;

4) Calculer le point  $P = h_1.G + h_2.W$  ;  
5) Calculer le point  $Z = h.W$  ;  
6) Pour  $j$  allant de 0 à  $2^{8t}-1$  ; exécuter les étapes suivantes:

- 5           6)a) Si  $P=0$ , exécuter l'étape 6)d) ;  
              6)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f_1=c-i$  modulo  $r$  ;  
              6)c) Retrouver le message  $m_1$  à partir de  $f_1$  et vérifier que  $f_1=R(m_1)$ ; si oui, exécuter l'étape  
10          8) ;  
              6)d) Remplacer  $P$  par  $P+Z$  ;  
7) La signature n'est pas valide et le procédé est terminé ;  
8) Si l'entier  $c=c'*2^{8t}+j$  n'appartient pas à  
15 l'intervalle  $[1,r-1]$ , la signature n'est pas valide, sinon la signature est valide et le procédé est terminé.

15- Procédé de modification du schéma de signature avec reconstitution partielle du message selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il consiste à remplacer la signature  $(c,d)$  par la signature  $(h_2,d)$  avec  $h_2=c*d^{-1}$  modulo  $r$ .

25 16- Procédé d'amélioration du schéma de signature de Nyberg-Rueppel, ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, ledit procédé consistant à inclure une partie du message de taille  $t$  octets dans l'entier  $d$ , la signature étant le couple d'entiers  $(c,d)$ ,  $t$  étant un entier petit, les  $t$  octets de poids faible de l'entier  $d$  contenant  $t$  octets du

message, ledit procédé utilisant un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté  $O$  et de générateur le point  $G$ , la clé privée étant un entier positif  $s$  inférieur à  $r$  et 5 la clé publique étant le point  $W=s.G$ , caractérisé en ce que le procédé de génération de la signature d'un message  $m$  utilisant les paramètres entiers  $t$ ,  $a$ , et  $k$  et comporte les 7 étapes suivantes :

10 1) Calculer  $h=H(m)$ ,  $H$  étant une fonction de hachage ;

2) Enlever les  $t$  octets de poids faible et les  $k$  octets de poids fort du message  $m$  et mémoriser le résultat dans  $m'$  ;

15 3) Mémoriser dans  $f$  le résultat de la concaténation à  $m'$  des  $a$  octets de poids fort de  $h$  ;

4) Générer un nombre aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$  ;

20 5) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f$  modulo  $r$  ; retourner à l'étape 4) si  $c=0$

6) Calculer l'entier  $d=u-s*c$  modulo  $r$  ; si  $d$  n'est pas égal à  $m$  modulo  $2^t$  retourner à l'étape 4) ;

7) La signature est le couple d'entiers  $(c,d)$  ;

25 et en ce que le procédé de vérification de la signature comporte les 7 étapes suivantes :

1) Si  $c$  n'appartient pas à l'intervalle  $[1,r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[0,r-1]$ , la 30 signature n'est pas valide ;

2) Calculer le point  $P=d.G+c.W$  ; si  $P=O$ , la signature n'est pas valide ;

- 3) Associer au point P l'entier i ;
- 4) Calculer l'entier  $f=c-i$  modulo r ;
- 5) Concaténer au message  $m'$ , obtenu à partir de f en enlevant les a octets de poids faible, les t octets de poids faible de d ;
- 6) Pour b allant de 0 à  $2^{8k}-1$  répéter l'étape suivante :
  - 6)a) Concaténer à b le message  $m'$  pour obtenir m et calculer  $h=H(m)$  ; vérifier que les a octets de poids fort de h et les a octets de poids faible de f sont identiques ; si oui, la signature du message m est valide et le procédé est terminé ;
- 7) La signature n'est pas valide.

15

17- Procédé de génération et de vérification de signature électronique selon l'une quelconque des revendications précédentes caractérisé en ce que les opérations s'effectuent sur une courbe elliptique formant une structure de groupe et possédant au moins un point G, qui est générateur d'un sous-groupe d'ordre un nombre premier r.

18- Procédé de génération et de vérification de signature électronique selon l'une quelconque des revendications précédentes caractérisé en ce que les opérations s'effectuent dans le groupe multiplicatif des entiers modulo un nombre premier p.

30 19- Procédé de génération et de vérification de signature électronique selon l'une quelconque des revendications précédentes caractérisé en ce que les

opérations s'effectuent dans un sous-groupe multiplicatif d'ordre un entier premier r du groupe multiplicatif des entiers modulo un nombre premier p avec r divisant p-1.

5

20- Dispositif électronique selon l'une quelconque des revendications précédentes caractérisé en ce que le dispositif effectuant le test est un dispositif portable.

10

21- Dispositif électronique selon l'une quelconque des revendications précédentes caractérisé en ce que le dispositif est une carte à puce.

15 22- Dispositif électronique selon l'une quelconque des revendications précédentes caractérisé en ce que le dispositif est une carte sans contact.

20 23- Dispositif électronique selon l'une quelconque des revendications précédentes caractérisé en ce que le dispositif est une carte PCMCIA.

25 24- Dispositif électronique selon l'une quelconque des revendications précédentes caractérisé en ce que le dispositif est un badge.

25- Dispositif électronique selon l'une quelconque des revendications précédentes caractérisé en ce que le dispositif est une montre intelligente.

30